

ルータでのWAN MACSECのトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トポロジ](#)

[トラブルシューティング対象のMACSECの概要](#)

[MACsecパケットフォーマット](#)

[WAN-MACSEC](#)

[WAN MACSECパケットフォーマット](#)

[WAN MACSECの用語](#)

[MACSEC Key Agreement Protocol\(MKA\)および暗号化の概要](#)

[事前共有キー](#)

[802.1x/EAP](#)

[WAN MACSECのトラブルシューティング](#)

[コンフィギュレーション](#)

[運用上の問題](#)

[関連情報](#)

概要

このドキュメントでは、Cisco IOS® XEルータの動作を理解し、トラブルシューティングするための基本的なWAN MACSECプロトコルについて説明します。

前提条件

要件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの情報は、ASR 1000、ISR 4000、Catalyst 8000ファミリなどのCisco IOS XEルータに固有のものです。特定のハードウェアおよびソフトウェアのMACSECサポートを探します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トポロジ



トポロジ ダイアグラム

トラブルシューティング対象のMACSECの概要

MACsecはIEEE 802.1AE標準ベースのレイヤ2ホップバイホップ暗号化で、AES-128暗号化を使用したメディアアクセス非依存プロトコルにデータ機密性、データ整合性、およびデータ生成元認証を提供します。MACsecを使用して保護できるのは、ホスト側リンク（ネットワークアクセスデバイスとPCやIP電話などのエンドポイントデバイス間のリンク）だけです。

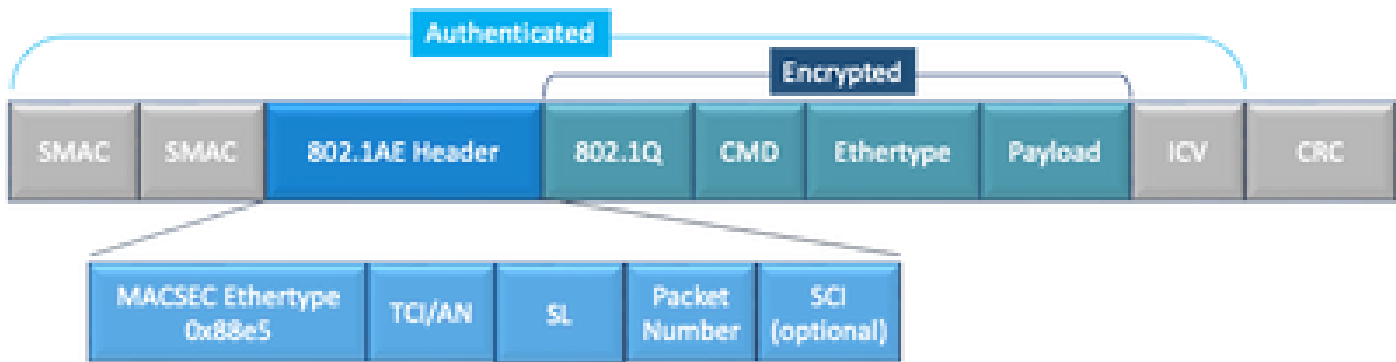
- 入力ポートでパケットが復号化されます。
- デバイス内のパケットはクリアです。
- パケットは出力ポートで暗号化されます。

MACsecは、有線LAN上で安全な通信を提供します。MACsecを使用してLAN上のエンドポイント間の通信を保護する場合、ワイヤ上の各パケットは対称キー暗号化を使用して暗号化されるため、ワイヤ上で通信の監視や変更を行うことはできません。MACsecをセキュリティグループタグ(SGT)と組み合わせて使用すると、フレームのペイロードに含まれるデータとともにタグが保護されます。

MACsecは、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上でMACレイヤの暗号化を提供します。

MACsecパケットフォーマット

802.1AE(MACsec)では、フレームはIP MTUまたはフラグメンテーションに影響を与えることなく、Integrity Check Value(ICV)で暗号化および保護され、最小L2 MTUへの影響は40バイト（ベージャイアントフレーム未満）です。



MACSECパケット形式の例

- MACsec EtherType:0x88e5。フレームがMACsecフレームであることを示します。
- TCI/AN：タグ制御情報/アソシエーション番号。機密性または整合性が単独で使用される場合のMACsecバージョン番号です。
- SL：暗号化データの長さ。
- PN：リプレイ保護に使用されるパケット番号。
- SCI：セキュアチャネル識別子。各接続アソシエーション(CA)は、仮想ポート（物理インターフェイスのMACアドレスと16ビットポートID）です。
- ICV: Integrity Check Value（整合性チェック値）

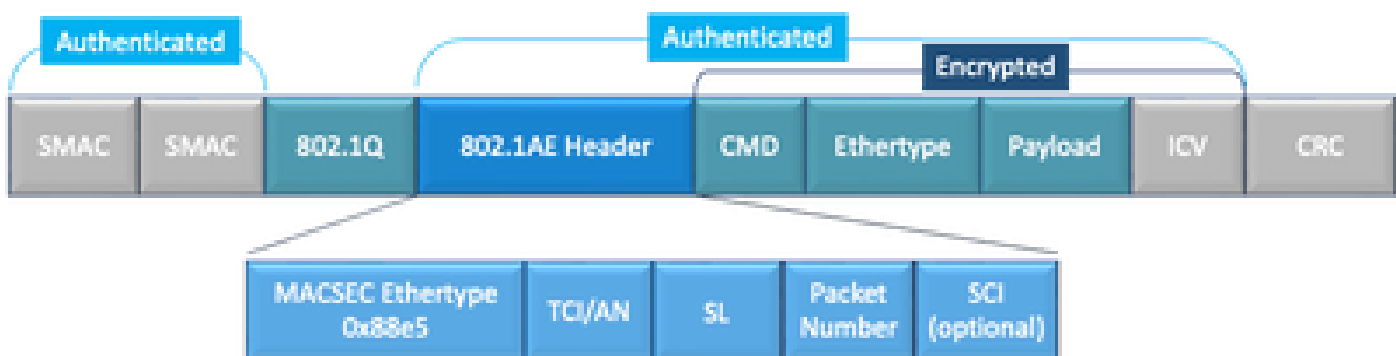
WAN-MACSEC

イーサネットは、プライベートLANトランスポートを超えて、さまざまなWANまたはMANトランスポートオプションを含むように進化しました。WAN MACSECは、AES 128または256ビットを使用して、ポイントツーポイントまたはポイントツーマルチポイントのレイヤ2イーサネット WANサービス全体でエンドツーエンドの暗号化を提供します。

WAN MACsecは(LAN)MACsecに基づいているため、IPsecとは別の名前になりますが、以前は利用できなかった追加機能がいくつか提供されています。

WAN MACSECパケットフォーマット

サービスプロバイダーがMACsec ethertypeをサポートしておらず、タグが暗号化されている場合にL2サービスを区別できない可能性があるため、WAN MACSECは802.1Qヘッダー以降のすべてのフレームを暗号化します。



クリアパケット形式のWAN MACSEC 802.1Qタグの例

新しい拡張機能の1つに、802.1Q Tags in the Clear (別名ClearTag) があります。この機能拡張により、802.1Qタグを暗号化されたMACsecヘッダーの外部に公開する機能が有効になります。このフィールドを公開すると、MACsecを使用した複数の設計オプションが提供されます。また、パブリックキャリアイーサネットトランスポートプロバイダーでは、特定のトランスポートサービスを活用するために必要です。

MKA機能のサポートにより、サービスプロバイダーがサービスの多重化を提供できるように、VLANタグ (802.1Qタグ) などのトンネリング情報がクリアテキストで提供されます。これにより、1つの物理インターフェイス上に複数のポイントツーポイントサービスまたはマルチポイントサービスを共存させ、現在表示されているVLAN IDに基づいて差別化できます。

サービスの多重化に加えて、クリアテキストのVLANタグにより、サービスプロバイダーは、802.1Qタグの一部として認識されるようになった802.1P(CoS)フィールドに基づいて、SPネットワーク上の暗号化されたイーサネットパケットにQuality of Service(QoS)を提供することもできます。

WAN MACSECの用語

MKA	IEEE 802.1XREV-2010 - Key Agreement Protocolで定義されているMACSec Key Agreement。MACSecピアの検出とキーのネゴシエーションに使用します。
MSK	EAP交換中に生成されるマスターセッションキー。サブリカントと認証サーバはMSKを使用してCAKを生成します
CAK	接続アソシエーションキーはMSKから取得されます。は、MACSecに使用される他のすべてのキーを生成するために使用される長寿命のマスターキーです。
CKN	Connectivity Association Key Name (接続アソシエーションキー名) :CAKを識別します。
サック	セキュアなアソシエーションキー : CAKから取得され、サブリカントとスイッチが特定のセッションのトラフィックを暗号化するために使用するキーです。
KS	キーサーバの役割 : <ul style="list-style-type: none"> • 暗号スイートの選択とアドバタイズ • CAKからのSAKの生成。
ケク	キー暗号化キー : MACsecキー(SAK)を保護するために使用されます。

MACSEC Key Agreement Protocol(MKA)および暗号化の概要

MKAは、WAN MACsecで使用されるコントロールプレーンメカニズムです。IEEE Std 802.1Xで規定されており、相互に認証されたMACsecピアと次のアクションを検出します。

- CA(Connectivity Association)を確立および管理します。
- ライブ/潜在的ピアリストを管理します。
- 暗号スイートのネゴシエーション

- CAのメンバの中からキーサーバ(KS)を選択します。
- Secure Association Key(SAK)の導出と管理。
- セキュアキーの配布。
- キーのインストール
- キー再生成.

設定済みのキーサーバの優先度 (最低) に基づいて、1つのメンバがキーサーバとして選出されます。KSの優先度がピア間で同じ場合は、最低のSCIが優先されます。

KSがSAKを生成するのは、可能性のあるすべてのピアが有効になり、少なくとも1つのライブピアが存在する場合だけです。MKA PDUまたはMKPDUを使用して、使用されるSAKと暗号を他の参加者に暗号化形式で配布します。

参加者は、SAKによって送信された暗号を確認し、サポートされている場合は、すべてのMKPDUでその暗号を使用して最新のキーを示してインストールします。サポートされていない場合は、SAKを拒否します

3ハートビート (各ハートビートはデフォルトで2秒) 後に参加者からMKPDUを受信しないと、ピアはライブピアリストから削除されます。たとえば、クライアントが切断された場合、クライアントから最後のMKPDUを受信してから3ハートビートが経過するまで、スイッチの参加者はMKAの操作を続行します。

このプロセスでは、暗号化キーを駆動する方法が2つあります。

- 事前共有キー
- 802.1x/EAP

事前共有キー

事前共有キーを使用する場合は、CAK=PSKおよびCKNを手動で入力する必要があります。キーライフタイムについては、キーのロールオーバーがあり、キー再生成の間にオーバーラップしていることを確認して、次のことを行います。

- 新しいSAKキーを交換してインストールし、アイドル状態のSAにバインドします。
- 古いSAKキーを消去し、新しいアイドルSAを割り当てます。

設定例 :

```
<#root>
```

```
key chain
```

```
  M_Key
```

```
    macsec
```

```
  key 01
```

```
    cryptographic-algorithm
```

```
    aes-128-cmac
```

```
key-string
12345678901234567890123456789001

lifetime 12:59:59 Oct 1 2023 duration 5000
key 02
cryptographic-algorithm aes-128-cmac
key-string 12345678901234567890123456789002
lifetime 14:00:00 Oct 1 2023 16:15:00 Oct 1 2023
key 03
cryptographic-algorithm aes-128-cmac
key-string 12345678901234567890123456789003
lifetime 16:15:00 Oct 1 2023 17:15:00 Oct 1 2023
key 04
cryptographic-algorithm aes-128-cmac
key-string 12345678901234567890123456789012
lifetime 17:00:00 Oct 1 2023 infinite
```

太字で示されている箇所は、次のとおりです。

M_Key : キーチェーン名。

キー01 : 接続関連キー名 (CKNと同じ)。

aes-128-cmac:MKA認証暗号。

12345678901234567890123456789012 : 接続アソシエーションキー(CAK)。


ポリシーの定義 :

<#root>

```
mka policy example
macsec-cipher-suite
```

```
gcm-aes-256
```


どこから? **gcm-aes-256**は、セキュアなアソシエーションキー(SAK)を導出するための暗号スイートを指します。

 注 : これは基本的なポリシー設定であり、confidentiality-offset、sak-rekey、include-icv-indicatorなどのより多くのオプションを使用できますが、実装によって異なります。

Interface:

```
interface TenGigabitEthernet0/1/2
mtu 2000
ip address 198.51.100.1 255.255.255.0
ip mtu 1468
eapol destination-address broadcast-address
```

```
mka policy example
mka pre-shared-key key-chain M_Key
macsec
end
```

 注:mkaポリシーが設定または適用されていない場合、デフォルトポリシーが有効になり、show mka default-policy detailで確認できます。

802.1x/EAP

EAP方式を使用する場合、すべてのキーはマスターセッションキー(MSK)から生成されます。IEEE 802.1X Extensible Authentication Protocol(EAP)フレームワークを使用すると、MKAはデバイス間でEAPoL-MKAフレームを交換します。EAPoLフレームのイーサタイプは0x888Eで、EAPoLプロトコルデータユニット(PDU)内のパケット本文はMACsec Key Agreement PDU(MKPDU)と呼ばれます。これらのEAPoLフレームには、送信側のCKN、キーサーバプライオリティ、およびMACsec機能が含まれています。

 注：デフォルトでは、スイッチはEAPoL-MKAフレームを処理しますが、転送しません。

証明書ベースのMACsec暗号化の設定例

証明書の登録 (認証局が必要) :

```
crypto pki trustpoint EXAMPLE-CA
  enrollment terminal
  subject-name CN=ASR1000@user.example, C=IN, ST=KA, OU=ENG,O=Example
  revocation-check none
  rsakeypair mkaioscarsa
  storage nvram:

crypto pki authenticate EXAMPLE-CA
```

必要な802.1x認証とAAA設定 :

```
aaa new-model
dot1x system-auth-control
radius server ISE
  address ipv4 auth-port 1645 acct-port 1646
  automate-tester username dummy
  key dummy123
  radius-server deadtime 2
!
aaa group server radius ISEGRP
  server name ISE
!
aaa authentication dot1x default group ISEGRP
aaa authorization network default group ISEGRP
```

EAP-TLSプロファイルおよび802.1Xクレデンシャル：

```
eap profile EAPTLS-PROF-IOSCA
method tls
pki-trustpoint EXAMPLE-CA
!
```

```
dot1x credentials EAPTLSCRED-IOSCA
username asr1000@user.example
pki-trustpoint EXAMPLE-CA
!
```

Interface:

```
interface TenGigabitEthernet0/1/2
macsec network-link
authentication periodic
authentication timer reauthenticate
access-session host-mode multi-host
access-session closed
access-session port-control auto
dot1x pae both
dot1x credentials EAPTLSCRED-IOSCA
dot1x supplicant eap profile EAPTLS-PROF-IOSCA
service-policy type control subscriber DOT1X_POLICY_RADIUS
```

WAN MACSECのトラブルシューティング

コンフィギュレーション

プラットフォームに応じて適切な設定と実装サポートを確認します。キーとパラメータが一致している必要があります。次に、設定に問題があるかどうかを特定する一般的なログをいくつか示します。

```
%MKA-3-INVALID_MACSEC_CAPABILITY : Terminating MKA Session because no peers had the required MACsec Cap
```

ピアのハードウェアのMACsec機能を確認するか、インターフェイスのMACsec設定を変更してMACsec機能の要件を下げます。

```
%MKA-3-INVALID_PARAM_SET : %s, Local-TxSCI %s, Peer-RxSCI %s, Audit-SessionID %s
```


設定やプラットフォームの異なるデフォルト設定に基づいて、ルータが予期するかしないいくつかのオプションのパラメータがあります。設定に含めるか、または廃棄してください。

%MKA-4-MKA_MACSEC_CIPHER_MISMATCH: Lower/Higher strength MKA-cipher than macsec-cipher for RxSCI %s, Au

ポリシー暗号スイートに設定の不一致があるため、適切に一致していることを確認します。

%MKA-3-MKPDU_VALIDATE_FAILURE : MKPDU validation failed for Local-TxSCI %s, Peer-RxSCI %s, Audit-Session

MKPDUが次の検証チェックの1つ以上に失敗しました：

- 有効なMACアドレスとEAPOLヘッダー：両方のインターフェイスの設定を確認してください。入カインターフェイスの packets capture は現在の値を裏付けることができます。
- 有効なCKNとアルゴリズムの俊敏性：有効なキーとアルゴリズムスイートを確認します。
- ICVの検証：ICVの検証はオプションのパラメータであり、設定の両端が一致している必要があります。
- MKAペイロードの正しい順序の存在：相互運用性の問題の可能性。
- ピアが存在する場合のMIの検証：メンバーIDの検証、参加者ごとに一意。
- ピアが存在する場合のMNの検証：メッセージ番号の検証。送信されるMKPDUごとに一意で、送信されるたびに増分されます。

運用上の問題

設定が完了すると、%MKA-5-SESSION_STARTメッセージが表示されますが、セッションが起動するかどうかを確認する必要があります。開始に適したコマンドは、show mka sessions [interface interface_name]です。

<#root>

Router1#

show mka sessions

```
Total MKA Sessions..... 1
Secured Sessions... 1
Pending Sessions... 0
```

```
=====
Interface      Local-TxSCI      Policy-Name      Inherited      Key-Server
Port-ID        Peer-RxSCI       MACsec-Peers     Status         CKN
=====
Te0/1/2        40b5.c133.0e8a/0012
```

Example

NO

NO

18 40b5.c133.020a/0012 1

Secured

01

Statusはコントロールプレーンセッションを示します。SecuredはRxおよびTx SAKがインストールされていることを示します。インストールされていない場合は、Not Securedとして表示されません。

- ステータスがInitのままである場合は、物理インターフェイスの状態、pingによるピアの接続、および設定の一致を確認します。この時点ではMKPDUが受信されず、ライブピアも存在しません。一部のプラットフォームではパディングが行われますが、他のプラットフォームでは行われません。最大32バイトのヘッダーオーバーヘッドを考慮して、適切な動作のために大きなMTUを確保してください。
- ステータスがPendingのままである場合は、MKPDUがコントロールプレーンの入力または出力でドロップされているか、あるいはインターフェイスのエラーまたはドロップを確認します。
- ステータスがNot Securedのままである場合、MKAインターフェイスはアップ状態で、MKPDUは通過していますが、SAKはインストールされていません。この場合、次のログが表示されます。

```
%MKA-5-SESSION_UNSECURED : MKA Session was not secured for Local-TxSCI %s, Peer-RxSCI %s, Audit-Session
```

これは、MACsecでのSecure Channel(SC)の確立とSecure Associations (SA ; セキュアアソシエーション) のインストールに先立って、MACsecサポートがないこと、無効なMACsec設定、またはローカルまたはピア側での他のMKA障害が原因です。show mka session [interface interface_name] detailの詳細については、detailコマンドを使用できます。

```
<#root>
```

```
Router1#
```

```
show mka sessions detail
```

```
MKA Detailed Status for MKA Session
```

```
=====
```

```
Status: SECURED - Secured MKA Session with MACsec
```

Local Tx-SCI..... 40b5.c133.0e8a/0012
Interface MAC Address.... 40b5.c133.0e8a
MKA Port Identifier..... 18
Interface Name..... TenGigabitEthernet0/1/2
Audit Session ID.....

CAK Name (CKN)..... 01

Member Identifier (MI)... DC5F7E3E38F4210925AAC8CA
Message Number (MN)..... 14462
EAP Role..... NA
Key Server..... NO

MKA Cipher Suite..... AES-128-CMAC

Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0
Latest SAK KI (KN)..... 272DA12A009CD0A3D313FADF00000001 (1)
Old SAK Status..... FIRST-SAK
Old SAK AN..... 0
Old SAK KI (KN)..... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)
SAK Rekey Time..... 0s (SAK Rekey interval not applicable)

MKA Policy Name..... Example
Key Server Priority..... 2
Delay Protection..... NO
Delay Protection Timer..... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility..... 80C201
SAK Rekey On Live Peer Loss..... NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation... NO
SAK Cipher Suite..... 0080C20001000002 (GCM-AES-256)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES

of MACsec Capable Live Peers..... 1
of MACsec Capable Live Peers Responded.. 0

Live Peers List:

MI	MN	Rx-SCI (Peer)	KS Priority	RxSA Installed	SSCI
272DA12A009CD0A3D313FADF	14712	40b5.c133.020a/0012	1	YES	0

Potential Peers List:

MI	MN	Rx-SCI (Peer)	KS Priority	RxSA Installed	SSCI
----	----	---------------	----------------	-------------------	------

状況をよりよく理解するために、強調表示されているピアと関連データのSAK情報を探します。
異なるSAKが設定されている場合は、使用されているキーとライフタイムまたは設定されている

SAKキー再生成オプションを調べます。事前共有キーが使用されている場合は、show mka keychainsを使用できます。

```
<#root>
```

```
Router1#
```

```
show mka keychains
```

```
MKA PSK Keychain(s) Summary...
```

Keychain Name	Latest CKN Latest CAK	Interface(s) Applied
---------------	--------------------------	-------------------------

```
=====
```

```
Master_Key
```

```
01
```

```
<HIDDEN>
```

```
Te0/1/2
```

CAKは表示されませんが、キーチェーン名とCKNを確認できます。

セッションは確立されているが、フラップまたは断続的なトラフィックフローが発生する場合は、MKPDUがピア間で正しくフローしているかどうかを確認する必要があります。タイムアウトが発生している場合は、次のメッセージを確認できます。

```
%MKA-4-KEEPALIVE_TIMEOUT : Keepalive Timeout for Local-TxSCI %s, Peer-RxSCI %s, Audit-SessionID %s, CKN
```

ピアが1つの場合、MKAセッションが終了します。複数のピアがあり、MKAが6秒以上いずれかのピアからMKPDUを受信しなかった場合、Live PeerはLive Peersリストから削除されます。show mka statistics [interface interface_name]から始めることができます。

```
<#root>
```

```
Router1#
```

```
show mka statistics interface TenGigabitEthernet0/1/2
```

```
MKA Statistics for Session
```

```
=====
```

```
Reauthentication Attempts.. 0
```

```
CA Statistics
```

```
Pairwise CAKs Derived... 0
```

```
Pairwise CAK Rekeys..... 0
```

```
Group CAKs Generated.... 0
Group CAKs Received..... 0
```

SA Statistics

```
SAKs Generated..... 0
SAKs Rekeyed..... 0
SAKs Received..... 1
SAK Responses Received.. 0
```

MKPDU Statistics

```
MKPDUs Validated & Rx... 11647
```

```
"Distributed SAK".. 1
"Distributed CAK".. 0
```

```
MKPDUs Transmitted..... 11648
```

```
"Distributed SAK".. 0
"Distributed CAK".. 0
```


送信および受信されるMKPDUは、1つのピアに対して同じ番号を持つ必要があります。RxとTxの両端で増加することを確認し、問題のある方向を判別または導きます。差異がある場合は、`debug mka linksec-interface frames`の両端を有効にできます。

```
*Sep 20 21:14:10.803: MKA-LLI-MKPDU: Received CKN length (2 bytes) from Peer with CKN 01
*Sep 20 21:14:10.803: MKA-LLI-MKPDU: MKPDU Received: Interface: [Te0/1/2 : 18] Peer MAC: 40:B5:C1:33:02
*Sep 20 21:14:12.101: MKA-LLI-MKPDU: MKPDU transmitted: Interface [Te0/1/2: 18] with CKN 01
*Sep 20 21:14:12.803: MKA-LLI-MKPDU: Received CKN length (2 bytes) from Peer with CKN 01
*Sep 20 21:14:12.803: MKA-LLI-MKPDU: MKPDU Received: Interface: [Te0/1/2 : 18] Peer MAC: 40:B5:C1:33:02
```

MKPDUを受信していない場合は、着信インターフェイスエラーまたはドロップ、ピアインターフェイスのステータス、およびmkaセッションを探します。両方のルータが送信しているが受信していない場合、MKPDUはメディアで失われ、正しい転送のために中間デバイスをチェックする必要があります。

MKPDUを送信していない場合は、物理インターフェイスの状態（回線およびエラー/ドロップ）と設定を確認します。コントロールプレーンレベルでこれらのパケットを生成しているかどうかを調べます。FIAトレースとEmbedded Packet Capture(EPC)はこの目的で信頼できるツールです。「[Cisco IOS XEデータパスパケットトレース機能によるトラブルシューティング](#)」を参照してください。

`debug mka events`を使用して、次のステップの指針となる理由を探することができます。

 注:debug mkaおよびdebug mka diagnosticsは、ルータ上でコントロールプレーンの問題を引き起こす可能性があるステートマシンと非常に詳細な情報を示すため、注意して使用してください。

セッションがセキュアで安定しているが、トラフィックが流れない場合は、両方のピアを送信する暗号化されたトラフィックを確認します。

<#root>

Router1#

show macsec statistics interface TenGigabitEthernet 0/1/2

MACsec Statistics for TenGigabitEthernet0/1/2

SecY Counters

Ingress Untag Pkts:	0
Ingress No Tag Pkts:	0
Ingress Bad Tag Pkts:	0
Ingress Unknown SCI Pkts:	0
Ingress No SCI Pkts:	0
Ingress Overrun Pkts:	0
Ingress Validated Octets:	0

Ingress Decrypted Octets: 98020

Egress Untag Pkts:	0
Egress Too Long Pkts:	0
Egress Protected Octets:	0

Egress Encrypted Octets: 98012

Controlled Port Counters

IF In Octets:	595380
IF In Packets:	5245
IF In Discard:	0
IF In Errors:	0
IF Out Octets:	596080
IF Out Packets:	5254
IF Out Errors:	0

Transmit SC Counters (SCI: 40B5C1330E8B0013)

Out Pkts Protected:	0
---------------------	---

Out Pkts Encrypted: 970

Transmit SA Counters (AN 0)

Out Pkts Protected:	0
---------------------	---

Out Pkts Encrypted: 970

Receive SA Counters (SCI: 40B5C133020B0013 AN 0)

In Pkts Unchecked:	0
In Pkts Delayed:	0

In Pkts OK: 967

In Pkts Invalid: 0

In Pkts Not Valid:	0
In Pkts Not using SA:	0
In Pkts Unused SA:	0
In Pkts Late:	0

SecYカウンタは物理インターフェイス上の現在のパケットですが、その他のカウンタはTx Secure Channelに関連しています。つまり、パケットが暗号化されて送信されていることを意味し、Rx Secured Associationはインターフェイスで受信された有効なパケットを意味します。

debug mka errorsやdebug mka packetsなどのその他のデバッグは、問題の特定に役立ちます。大量のロギングを引き起こす可能性があるため、この最後のデバッグは予防策として使用してください。

関連情報

- [MACsecおよびMKA設定ガイド](#)
- [シスコテクニカルサポートおよびダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。